UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

JANE DOE, on behalf of herself and all others similarly situated, Plaintiff, v. **CURIUM US LLC D/B/A CURIUM PHARMA**, Defendant.	Case No. 4:25-cv-00964 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff JANE DOE ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant CURIUM US LLC d/b/a CURIUM PHARMA ("Curium Pharma" or "Defendant") individually, on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack discovered by Defendant on October 17, 2024, resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Breach occurred between October 15, 2024, and October 19, 2024, but was not discovered by Defendant until October 17, 2024, two days after the breach had first begun and at least two days before the breach stopped.

3. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former employees' highly personal information, including names, Social Security

Numbers, driver's license, ("personally identifying information" or "PII"), and medical information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

4. On or about June 20, 2025–a month after the Data Breach was discovered– Curium Pharma finally began notifying Plaintiff and the Class of the Breach through breach notices ("Breach Notice"). Plaintiff's breach notice is attached as Exhibit A.

5. Defendant took eight months before informing Class Members even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. Curium Pharma's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell employees how many people were impacted, how the breach happened, and why it took Defendant until June 20, 2025, to begin notifying victims that hackers had gained access to highly private Sensitive Information between October 15, 2024, and October 19, 2024.

7. Defendant's failure to timely detect and report the Data Breach made its employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach,

Defendant violated state and federal law and harmed thousands of its current and former employees.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a former employee and Data Breach victim.

12. Accordingly, Plaintiff, on behalf of herself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Jane Doe is a natural person and citizen of Whiteland, Indiana, where she intends to remain.

14. Defendant Curium Pharma is a Delaware corporation with its principal place of business located at 111 West Port Plaza Drive, Suite 800, St. Louis, Missouri 63146.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendant are of different states. And there are over 100 putative Class members.

16. This Court has personal jurisdiction over Defendant because it is headquartered in Missouri, regularly conducts business in Missouri, and has sufficient minimum contacts in Missouri.

17. Venue is proper in this Court because Defendant's principal offices are in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

STATEMENT OF FACTS

Curium Pharma

18. Curium Pharma touts that its purpose is to "develop, manufacture, and supply world-class radiopharmaceutical products around the globe."[1] With offices across the country and a global presence, Curium Pharma touts an annual revenue of 675.1 billion.[2]

19. In collecting and maintaining its current and former employees' Sensitive Information, Curium Pharma agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information.

20. Indeed, Curium Pharma promises in its privacy policy that "The Site uses state-of-the-art technology to keep any information you provide as secure as possible."[3]

21. Despite recognizing its duty to do so, on information and belief, Curium Pharma has not implemented reasonably cybersecurity safeguards or policies to protect its employees' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect,

[1] About us, https://www.curiumpharma.com/about/who-we-are/ (last visited June 30, 2025).
[2] RocketReach, https://rocketreach.co/curium-pharma-profile_b44cd081fd63eaaa (last visited June 30, 2025).
[3] Curium Pharma, Privacy policy, https://www.curiumpharma.com/privacy/ (last visited June 30, 2025).

and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' Sensitive Information.

The Data Breach

22. Plaintiff is a former Curium Pharma employee and a Data Breach victim. As a condition of treatment with Defendant, Plaintiff provided it with her Sensitive Information including her name, Social Security Number, driver's license information, and medical records. Curium Pharma used Sensitive Information to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that Sensitive Information to obtain employment.

23. On information and belief, Defendant collects and maintains employees' Sensitive Information in its computer systems.

24. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

25. According to the online Breach Notice, Defendant admits that, between October 17, 2024, "IT staff for Curium Pharma identified suspicious activity within our network." Following an internal investigation, Curium Pharma discovered that an "unauthorized party was able to access some data in our systems between October 15, 2024, and October 19, 2024." Ex. A.

26. In other words, Defendant's cyber and data security systems were so completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees highly private Sensitive Information for several weeks. Further, Defendant had been completely unable to detect this breach until an appalling nine months later.

27. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

28. On or around June 20, 2025– *eight* months after the Breach first begun– Curium Pharma finally notified Plaintiff and Class Members about the Data Breach.

29. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing employees' Sensitive Information, as evidenced by the Data Breach.

30. In response to the Data Breach, Defendant contends that it will implement "additional safeguards and security." Ex. A. Although Defendant fails to expand on what these alleged "additional safeguards and security" are, such steps should have been in place before the Data Breach.

31. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." Ex. A.

32. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect employees' Sensitive Information, insisting that, despite the Data Breach demonstrating otherwise, it wanted to "assure you that we take it seriously." Ex. A.

33. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

34. On information and belief, Curium Pharma has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

35. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

36. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

37. It is well known that Sensitive Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

38. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[4]

39. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records,

[4] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 4, 2023).

March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

41. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Sensitive Information private and secure, Defendants failed to take appropriate steps to protect the Sensitive Information of Plaintiff and Class Members from being compromised.

42. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

43. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[5]

44. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive

[5] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed September 4, 2023).

in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[6]

45. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

46. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) ransomware actors were targeting entities such as Defendants, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendants, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

47. In light of the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted Sensitive Information of thousands of its current and former employes in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Sensitive Information and Defendants' type of business had cause to be particularly on guard against such an attack.

48. Before the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Sensitive Information could be accessed,

---

[6] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed September 4, 2023).

[7] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed September 4, 2023).

exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendants.

49. Prior to the Data Breach, Defendants knew or should have known that it should have encrypted their employees' Social Security numbers and other sensitive data elements within the Sensitive Information to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience

50. Plaintiff is a former Curium Pharma employee and a Data Breach victim. As a condition of treatment with Defendant, Plaintiff provided it with her Sensitive Information including her name, Social Security Number, driver's license information, and medical records. Curium Pharma used Sensitive Information to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that Sensitive Information to obtain employment.

51. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her.

52. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

53. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

54. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

55. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

56. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

57. Plaintiff have suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

58. Plaintiff suffered actual injury from the exposure of her Sensitive Information—which violates her rights to privacy.

59. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

60. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

61. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

63. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

64. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals

frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

66. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

67. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

69. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive

and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

70. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

71. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[8] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[9]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[10]

c. 89% of consumers stated that "I care about data privacy."[11]

[8] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[9] *Id*. at 3.
[10] *Id*.
[11] *Id*. at 9.

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[12]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[13]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[14]

72. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Sensitive Information, including Plaintiff and the Class's Sensitive Information, was important to its employees.

Defendant failed to adhere to FTC guidelines.

73. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

[12] *Id*.
[13] *Id*.
[14] *Id*. at 11.

e. implement policies to correct security problems.

75. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

76. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

79. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep employees' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [15]

80. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[16]

81. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or

[15] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[16] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

82. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

83. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

84. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

85. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

86. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

87. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

88. Plaintiff brings this class action individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach, including all those who received notice of the breach.

89. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

92. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff realleges all previous paragraphs as if fully set forth below.

94. Plaintiff and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

95. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Sensitive Information.

98. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

99. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

100. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

101. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face. .

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

102. Plaintiff realleges all previous paragraphs as if fully set forth below.

103. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

105. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

106. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

107. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

108. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

109. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

111. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

112. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

113. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

114. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

115. Defendant's various violations and its failure to comply with applicable laws and regulations constitute negligence *per se*.

116. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of

Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

117. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

118. Plaintiff realleges all previous paragraphs as if fully set forth below.

119. Plaintiff and the Class delivered their Sensitive Information to Defendant as part of the process of obtaining employment provided by Defendant.

120. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

121. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

122. In delivering their Sensitive Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

123. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

124. Defendant accepted possession of Plaintiff's and Class Members' Sensitive Information.

125. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure employees' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

126. Defendant recognized that employees' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

127. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

128. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

129. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

130. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information;

(c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

131. Plaintiff realleges all previous paragraphs as if fully set forth below.

132. This claim is pleaded in the alternative to the breach of contractual duty claim.

133. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

134. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

135. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have

provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

136. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

137. Plaintiff realleges all previous paragraphs as if fully set forth below.

138. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

139. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

140. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Sensitive Information is highly offensive to a reasonable person.

141. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

142. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

143. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

144. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

145. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

146. As a proximate result of Defendant's acts and omissions, the Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

147. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their Sensitive Information are still maintained by Defendant with its inadequate cybersecurity system and policies.

148. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiff and the Class.

149. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which

includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: June 30, 2025

By: */s/ Raina C. Borrelli*

Raina C. Borrelli*
Samuel J. Strauss*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

**Pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class